VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN PRÜFUNG BEAUFTRAGTE BEHÖRDE

An:

SONN & PARTNER
Riemergasse 14
A-1010 Wien
AUTRICHE

MITTEILUNG ÜBER DIE ÜBERSENDUNG DES INTERNATIONALEN VORLÄUFIGEN PRÜFUNGSBERICHTS

(Regel 71.1 PCT)

Absendedatum *(Tag/Monat/Jahr)*	16.12.2004
Aktenzeichen des Anmelders oder Anwalts: R 42658	**WICHTIGE MITTEILUNG**

Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/AT 03/00351	21.11.2003	22.11.2002

Anmelder: ARC SEIBERSDORF RESEARCH GMBH et al.

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Prüfungsbericht, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.

2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.

3. Auf Wunsch eines ausgewählten Amts wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.

4. **ERINNERUNG**

   Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

   Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Prüfungsbericht enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

   Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

   Der Anmelder wird auf Artikel 33(5) hingewiesen, in welchem erklärt wird, daß die Kriterien für Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit, die im Artikel 33(2) bis (4) beschrieben werden, nur für die internationale vorläufige Prüfung Bedeutung haben, und daß "jeder Vertragsstaat (...) für die Entscheidung über die Patentfähigkeit der beanspruchten Erfindung in diesem Staat zusätzliche oder abweichende Merkmale aufstellen" kann (siehe auch Artikel 27(5)). Solche zusätzlichen Merkmale können z.B. Ausnahmen von der Patentierbarkeit, Erfordernisse für die Offenbarung der Erfindung sowie Klarheit und Stützung der Ansprüche betreffen.

Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde	Bevollmächtigter Bediensteter
Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Emery, C Tel. +31 70 340-2848

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESE

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts R 42658	**WEITERES VORGEHEN** siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/AT 03/00351	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 21.11.2003	Prioritätsdatum *(Tag/Monat/Jahr)* 22.11.2002
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/08		
Anmelder ARC SEIBERSDORF RESEARCH GMBH et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 2 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Bescheids
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Regel 66.2 a)ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
16.06.2004	16.12.2004
Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Bevollmächtigter Bediensteter Liebhardt, I Tel. +31 70 340-4114

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/AT 03/00351

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung *(Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17))*:

Beschreibung, Seiten

1-24	in der ursprünglich eingereichten Fassung

Ansprüche, Nr.

6 (Teil), 7-10	eingegangen am 19.06.2004 mit Schreiben vom 16.06.2004
1-5, 6 (Teil)	eingegangen am 11.11.2004 mit Schreiben vom 09.11.2004

Zeichnungen, Blätter

1/11-11/11	in der ursprünglich eingereichten Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um:

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).

   ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

   ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:

   ☐ Ansprüche, Nr.:

   ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen.)

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-10
	Nein:	Ansprüche	
Erfinderische Tätigkeit (IS)	Ja:	Ansprüche	1-10
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (IA)	Ja:	Ansprüche:	1-10
	Nein:	Ansprüche:	

2. Unterlagen und Erklärungen:

   siehe Beiblatt

Zu Punkt V

Begründete Feststellung hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

Es wird auf das folgende Dokument verwiesen:

D1: ELLIOTT C: "Building the quantum network" NEW JOURNAL OF PHYSICS, 2002, DEUTSCHE PHYSIKALISCHE GESELLSCHAFT & IOP PUBLISHING LTD, UK, Bd. 4, 12. Juli 2002 (2002-07-12), Seiten 46.1-46.12, XP002271991 ISSN: 1367-2630

1. Das Dokument D1 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des Anspruchs 1 angesehen. Es offenbart ein Kommunikationssystem mit Quantenkryptographie (Seite 46.8, Zeilen 15-26), mit an Quantenkanälen angeschlossenen *Endvermittlungsstationen* (Fig. 5, "QKD Endpoint") und den Quantenkanälen zugeordneten quantenkryptographischen Einrichtungen zur Generierung eines Quanten-Schlüssels (Seite 46.9, Zeilen 5 und 6), und mit mehreren miteinander verbundenen Vermittlungsstationen (Fig. 5, "Trusted Relay") wobei die Vermittlungsstationen über öffentliche Leitungen unter Anwendung von vereinbarter Verschlüsselung miteinander kommunizieren (Fig. 5, obere, weiße Pfeile und Seite 46.9, Zeilen 20-24), und daß die *Endvermittlungsstationen* ihrerseits mit den Vermittlungsstationen über die Quantenkanäle zur Generierung eines jeweiligen temporären Quanten-Schlüssels verbunden, und weiters zur Kommunikation über öffentliche Leitungen unter Verwendung des über die Vermittlungsstationen generierten Quanten-Schlüssels eingerichtet sind (Seite 46.9, Zeilen 20-24).

1.1. Der Gegenstand des Anspruchs 1 unterscheidet sich daher von dem bekannten Kommunikationssystem dadurch, daß die *Teilnehmerstationen* ***direkt*** an die Quantenkanäle angeschlossen sind und dadurch, daß die Vermittlungsstationen untereinander über öffentliche Leitungen unter Anwendung von vereinbarter Verschlüsselung *ohne quantenkryptographischen Schlüsselaustausch* kommunizieren.

Der Gegenstand des Anspruchs 1 ist somit neu (Artikel 33(2) PCT).

1.2. Die mit der vorliegenden Erfindung zu lösende Aufgabe kann somit darin gesehen werden, daß zum einen die durch die Quantenkryptographie gewährleistete hohe Sicherheit bis zum Endbenutzer hin erstreckt und zum anderen das Gesamtsystem durch die Verminderung der Anzahl von Vermittlungsstationen ökonomischer gestaltet werden soll.

Die in Anspruch 1 der vorliegenden Anmeldung für diese Aufgabe vorgeschlagene Lösung beruht aus den folgenden Gründen auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT):

Die Aufgabenstellung der Erstreckung der besonders sicheren Quantenkryptographie bis hin zu den Endbenutzern findet im Dokument D1 keine Erwähnung. Zwar wird die Aufwendigkeit der Vermittlungsstationen in D1 angesprochen; es gibt jedoch keinen Hinweis auf die ökonomischere Gestaltung des Gesamtsystems durch die Ausführung der Kommunikation der Vermittlungsstationen untereinander über öffentliche Leitungen unter Anwendung von vereinbarter Verschlüsselung ohne quantenkryptographischen Schlüsselaustausch.

2. Die Ansprüche 2-10 sind vom Anspruch 1 abhängig und erfüllen damit ebenfalls die Erfordernisse des PCT in bezug auf Neuheit und erfinderische Tätigkeit.

Patentansprüche

1. Kommunikationssystem mit Quantenkryptographie, mit an Quantenkanäle (3) angeschlossenen Teilnehmerstationen (1.i, 2.i) und den Quantenkanälen zugeordneten quantenkryptographischen Einrichtungen (10, 11) zur Generierung eines Quanten-Schlüssels, und mit mehrere miteinander verbundenen Vermittlungsstationen (1, 2) dadurch gekennzeichnet, dass die Vermittlungsstationen (1, 2) über öffentliche Leitungen unter Anwendung von vereinbarter Verschlüsselung, ohne quantenkryptographischen Schlüsselaustausch, miteinander kommunizieren, und dass die Teilnehmerstationen (1.i, 2.i) ihrerseits mit den Vermittlungsstationen (1, 2) über die Quantenkanäle (3) zur Generierung eines jeweiligen temporären Quanten-Schlüssels verbunden, und weiters zur Kommunikation über öffentliche Leitungen (4) unter Verwendung des über die Vermittlungsstationen (1, 2) generierten Quanten-Schlüssels eingerichtet sind.

2. Kommunikationssystem nach Anspruch 1, dadurch gekennzeichnet, dass die Vermittlungsstationen (1, 2) als quantenkryptographische Einrichtung eine Photonenquelle (10) sowie für den Fall der Verwendung von verschränkten Photonen auch einen Photonendetektor (11) enthalten.

3. Kommunikationssystem nach Anspruch 2, dadurch gekennzeichnet, dass die Teilnehmerstationen (1.i, 2.i) nur eine Photonen-Detektionseinrichtung (11') enthalten.

4. Kommunikationssystem nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Vermittlungsstationen (1, 2, 6', 7') zumindest teilweise in Form von Punkt-zu-Punkt-Verbindungen miteinander verbunden sind.

5. Kommunikationssystem nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Vermittlungsstationen (1, 2, 6-9) zumindest teilweise hierarchisch miteinander verbunden sind.

6. Kommunikationssystem nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass nach einer über die jeweilige Vermittlungsstation (1, 2) übermittelten Kommunikations-Aufforde-

rung die an der gewünschten Kommunikation beteiligten Teilnehmerstationen (1.1, 2.1) jeweils mit ihrer zugehörigen Vermittlungsstation (1, 2) über den Quantenkanal (3) eine gesonderte Schlüssel-Bitfolge erzeugen.

7. Kommunikationssystem nach Anspruch 6, dadurch gekennzeichnet, dass die der gerufenen Teilnehmerstation (2.1) zugehörige Vermittlungsstation (2) aus den über die Quantenkanäle (3) erzeugten Schlüssel-Bitfolgen eine dritte Schlüssel-Bitfolge erzeugt und zur gerufenen Teilnehmerstation (2.1) übermittelt, die hieraus unter Verwendung der ihr bekannten, von ihr zusammen mit der zugehörigen Vermittlungsstation erzeugten Schlüssel-Bitfolge die auf Seiten der rufenden Teilnehmerstation (1.1) erzeugte Schlüssel-Bitfolge erzeugt, die dann endgültig als gemeinsamer Schlüssel für die Kommunikation zwischen den Teilnehmerstationen (1.1, 2.1) verwendet wird.

8. Kommunikationssystem nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass bei Beenden der Kommunikation der für diese Kommunikation generierte Quanten-Schlüssel verworfen wird.

9. Kommunikationssystem nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass der generierte Quanten-Schlüssel auf Störungsfreiheit überprüft wird, und dass auf eine etwaige erfasste Störung hin, die einem Abhören zugeordnet wird, der Kommunikationsaufbau abgebrochen und der Schlüssel verworfen wird.

10. Kommunikationssystem nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass vor dem Aufbau einer Kommunikation zwischen Teilnehmerstationen (1.1, 2.1) von diesen an die jeweils zugehörige Vermittlungsstation (1, 2) übermittelte, für sie spezifische Daten, wie z.B. Authentifikationsdaten, von der jeweiligen Vermittlungsstation überprüft werden.